Tipp von Kursleiter Markus Hengstler

Troubleshooting Kerberos-Authentisierung



Seit der Einführung von Windows 2000 und damit Active Directory ist Kerberos das Standard-Authentisierungsverfahren. Die älteren Protokolle NTLM und NTLMv2 werden allerdings immer noch unterstützt, da eventuell nicht alle Clients mit Kerberos umgehen können. Es ist daher nicht erstaunlich, dass viele Administratoren glauben, in ihrer Umgebung werde Kerberos verwendet, dies aber aus diversen Gründen nicht der Fall ist. In Wirklichkeit findet ein Fallback zu NTLM statt. Kerberos bietet aber einige Vorteile:

- Single Sign-on möglich
- Bessere Performance als NTLM

In diesem Artikel möchte ich einerseits grob erklären, wie Kerberos funktioniert und welche Voraussetzungen erfüllt sein müssen, andererseits auch zeigen, welche Mittel für das Troubleshooting zur Verfügung stehen.

Die Authentisierung

Generell wird die Authentisierung immer durchgeführt, wenn ein User oder Computer auf eine Ressource zugreifen will. Es muss festgestellt werden, wer den Zugriff durchführen will, bevor anhand von Berechtigungen geprüft werden kann, ob die Aktion erlaubt ist. Authentisierung und Autorisierung sind immer separate Prozesse.

Die Identität wird in Active Directory mittels Security Identifier (SID) verwaltet. Jeder Account – ob User oder Computer – hat eine SID (nach Migrationen eventuell sogar mehrere). Der Befehl WhoAmI zeigt diese SID des angemeldeten Benutzers an:

```
C:\Users\markus.hengstler>whoami /user

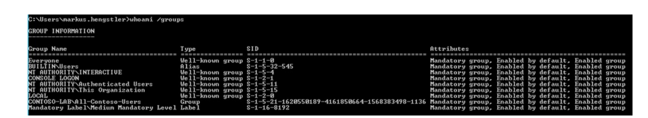
USER INFORMATION
----------------

User Name                    SID
============================ ==============================================
contoso-lab\markus.hengstler S-1-5-21-1620550189-4161850664-1568383498-1135
```

WhoAmI zeigt die SID des angemeldeten Benutzers

Jede Gruppe, der ein Benutzer angehört, hat ebenfalls eine SID. Bei der Anmeldung werden alle Gruppen- und die Benutzer-SID zusammengefasst und in ein Access Token geschrieben. Dieses kann dann für die Autorisierung verwendet werden. Genauer: Es wird jedem Prozess, der gestartet wird, angehängt und beim Zugriff auf Ressourcen wie Dateien oder Ordner mit den SIDs in den Access Control Lists (ACL) verglichen.

Auch die Gruppen-SID kann mit WhoAmI überprüft werden:



Überprüfen der Gruppen-SID mit WhoAmI

Woher stammen nun die Informationen? Sie werden von der lokalen Sicherheitsautorität und der Domäne zur Verfügung gestellt. Die Domänen-SIDs (In den Screenshots



0844 844 822, info@digicomp.ch, www.digicomp.ch

190913

diejenigen mit der langen Nummer) bekommt der Benutzer im Rahmen der Authentisierung vom Domain Controller mitgeteilt. Dazu muss der Benutzer aber erst glaubhaft machen, dass er derjenige ist, den er vorgibt zu sein.

Wie funktioniert Kerberos?

Für Kerberos läuft der Authentisierungsprozess wie folgt ab:

- Der Benutzer verbindet sich mit einem speziellen Service auf einem Domain Controller – dem Key Distribution Center (KDC) – über Port TCP88 und verlangt vom Authentication Service (AS) ein Ticket Granting Ticket (TGT). Der Request beinhaltet auch Daten, die mit dem User Key verschlüsselt sind. Da der User Key mit dem Passwort des Benutzers erstellt wurde, kann der DC verifizieren, dass der Sender des Requests dieses Passwort wirklich gekannt hat. Im Screenshot ist ersichtlich, dass für den Benutzer markus.hengstler in der Domäne CONTOSO-LAB für den Service Kerberos TGT ein Ticket angefordert und ausgestellt wurde. Das Ticket beinhaltet einen Session Key, der für die Kommunikation mit dem Ticket Granting Service (TGS) verwendet werden kann – einmal verschlüsselt mit dem User Key und einmal mit dem Key des Services selbst.



1122	37.1333988	CON-RED-O20...	con-red-dc1.c...	KerberosV5	KerberosV5:AS Request Cname: markus.hengstler Realm: CONTOSO-LAB Sname: krbtgt/CONTOSO-LAB
1123	37.1339141	con-red-dc1.c...	CON-RED-O20...	KerberosV5	KerberosV5:KRB_ERROR - KDC_ERR_PREAUTH_REQUIRED (25)
1131	37.1703273	CON-RED-O20...	con-red-dc1.c...	KerberosV5	KerberosV5:AS Request Cname: markus.hengstler Realm: CONTOSO-LAB Sname: krbtgt/CONTOSO-LAB
1132	37.1710878	con-red-dc1.c...	CON-RED-O20...	KerberosV5	KerberosV5:AS Response Ticket[Realm: CONTOSO-LAB.COM, Sname: krbtgt/CONTOSO-LAB.COM]

- Der Benutzer verbindet sich abermals zum KDC und fordert mit Hilfe des Session Keys vom TGS ein Service-Ticket (ST) an. Dies kann für einen Dateizugriff übers Netz, Zugriff auf einen Webserver im internen Netz oder wie im Beispiel für eine Anmeldung an einer Workstation sein.

1140	37.1732062	CON-RED-O20...	con-red-dc1.c...	KerberosV5	KerberosV5:TGS Request Realm: CONTOSO-LAB.COM
1143	37.1739377	con-red-dc1.c...	CON-RED-O20...	KerberosV5	KerberosV5:TGS Response Cname: markus.hengstler

- Der Service-Name ist der sogenannte Service Principal Name (SPN), der aus Service/FQDN besteht. Im Beispiel unten host/con-red-O2010 – eine Workstation.

```
ReqBody:
  SequenceHeader:
  Tag0:
  KdcOptions: 0x40810000
  Tag2: 0x1
  Realm: CONTOSO-LAB.COM
  Tag3:
  Sname: host/con-red-o2010.contoso-la/NULL
```

- Das Service-Ticket beinhaltet einen Session Key zwischen Benutzer und dem Service, jeweils verschlüsselt mit deren eigenem Key.
- Mit dem Service-Ticket verbindet sich der Benutzer mit dem Service. Er schickt einen Datensatz (Authenticator) mit – verschlüsselt mit dem Session Key. Der Service selbst hat den Session Key ebenfalls zur Verfügung und kann damit bestätigen, dass der Benutzer diesen erfolgreich aus dem Ticket extrahieren konnte und deshalb authentisch sein muss.

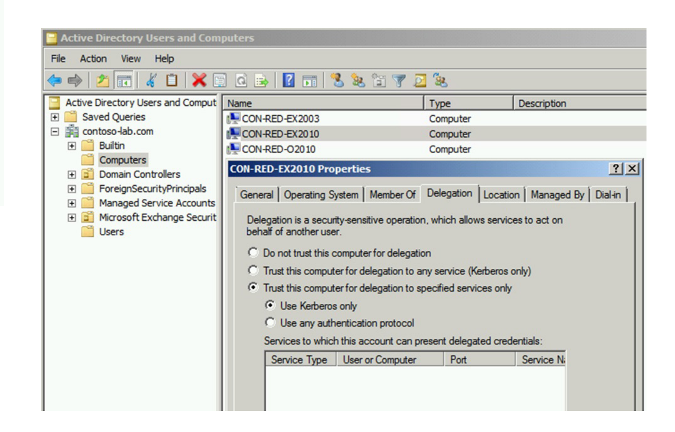
Optional kann der Benutzer auch eine Authentisierung des Services verlangen (Mutual Authentication). Dann schickt der Server ebenfalls einen Authenticator, den der Benutzer verifizieren kann.

Wieso wird ein zweistufiger Prozess mit TGT und ST verwendet? Nach Erhalt des TGT muss der Benutzer sein Passwort nicht mehr eingeben. Mit dem TGT beweist er gegenüber dem TGS, dass seine Identität schon geprüft worden ist. Sowohl TGT als auch ST haben eine Gültigkeitsdauer von 10 Stunden, wobei dies konfigurierbar ist.

Voraussetzungen für eine erfolgreiche Authentisierung mit Kerberos

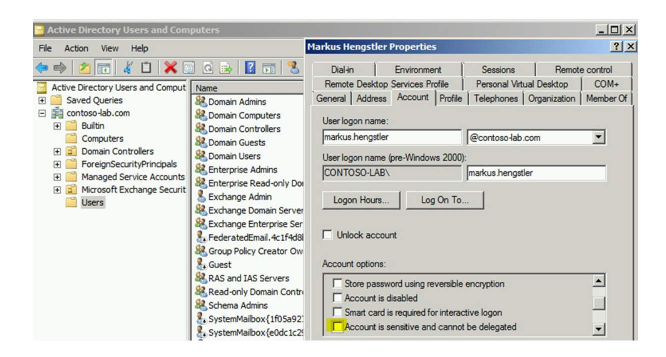
Damit Kerberos erfolgreich ist und kein Fallback auf NTLM erfolgt, müssen folgende Voraussetzungen erfüllt sein:

- Der Service Principal Name muss registriert und eindeutig sein. Oft verhindern Duplikate eine Authentisierung, wenn manuell SPNs hinzugefügt worden sind.
- Der Client muss den FQDN im Service Principal Name für die Verbindung benutzen. Gerade wenn Loadbalancer verwendet werden, ist zusätzliche Konfiguration nötig, da der SPN nur für ein Computeraccount registriert werden kann. In Exchange wird das Problem mit einem «virtuellen» Computeraccount gelöst – ähnlich wie bei Failover Clustering.
- Alle Parteien müssen die gleichen Verschlüsselungsalgorithmen für Kerberos-Tickets unterstützen. Ab Windows 7 und Windows Server 2008 R2 wird zum Beispiel DES standardmässig nicht mehr zugelassen. Dies muss für alte Clients oder Applikationen per Gruppenrichtlinie übersteuert werden.
- Für Szenarien, in denen sich ein Service gegenüber einem anderen Service als Benutzer ausgeben muss (Constraint Delegation, z.B. Webapplikation mit Zugriff auf eine SQL-Datenbank), müssen sowohl für den Service, der den Benutzer verkörpert, als auch für den Benutzer selbst die Delegation zugelassen sein:





0844 844 822, info@digicomp.ch, www.digicomp.ch



Troubleshooting-Tools für Kerberos

Natürlich kann für Kerberos-Troubleshooting wie für die Screenshots in obigem Beispiel Microsofts Netzwerk Monitor oder ein vergleichbares Analyse-Tool wie Wireshark verwendet werden. Mit den entsprechenden Filtern lässt sich die Konversation zwischen Client, Domain Controller und Zielserver verfolgen:

Gewisse Fehler lassen sich so einfach aufdecken:

- Falsche Service Principal Names
- Keine Kerberos-Kommunikation möglich wegen Firewalls
- Verschlüsselungstyp für Kerberos-Ticket wird von einer Partei nicht unterstützt

Für andere Fälle ist es hilfreich, die ausgestellten Kerberos-Tickets auf dem Client zu untersuchen oder die gespeicherten Tickets zu löschen, damit sie neu erstellt werden müssen. Dazu kann das Tool Klist verwendet werden, das ab Windows 7 und Windows Server 2008 R2 eingebaut ist.

```
C:\Users\markus.hengstler>klist

Current LogonId is 0:0x19885

Cached Tickets: (6)

#0>     Client: markus.hengstler @ CONTOSO-LAB.COM
        Server: krbtgt/CONTOSO-LAB.COM @ CONTOSO-LAB.COM
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x60a00000 -> forwarded renewable pre_authent
        Start Time: 11/18/2013 17:54:34 (local)
        End Time:   11/18/2013 23:41:24 (local)
        Renew Time: 11/25/2013 3:56:24 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

#1>     Client: markus.hengstler @ CONTOSO-LAB.COM
        Server: krbtgt/CONTOSO-LAB.COM @ CONTOSO-LAB.COM
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 11/18/2013 13:41:24 (local)
        End Time:   11/18/2013 23:41:24 (local)
        Renew Time: 11/25/2013 3:56:24 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

#2>     Client: markus.hengstler @ CONTOSO-LAB.COM
        Server: cifs/con-red-ex2010.contoso-lab.com @ CONTOSO-LAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/18/2013 19:30:12 (local)
        End Time:   11/18/2013 23:41:24 (local)
        Renew Time: 11/25/2013 3:56:24 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

Mit dem Befehl Klist purge lassen sich alle Tickets löschen.

```
C:\Users\markus.hengstler>klist purge

Current LogonId is 0:0x19885
        Deleting all tickets:
        Ticket(s) purged!
```

Zur Anzeige der Service Principal Names empfiehlt sich der Befehl setspn. Mit ihm lassen sich nicht nur SPNs erstellen und anzeigen, sondern auch nach doppelten suchen. Dies ist ein häufiges Problem, wenn manuell Namen hinzugefügt werden müssen. Jeder SPN muss eindeutig sein.
Der Befehl setspn –Q */con-red-ex2010.contoso-lab.com zum Beispiel zeigt alle SPNs des Hosts con-red-ex2010 an:

```
C:\Users\Administrator>setspn -Q */con-red-ex2010.contoso-lab.com
Checking domain DC=contoso-lab,DC=com
CN=CON-RED-EX2010,CN=Computers,DC=contoso-lab,DC=com
        POP/CON-RED-EX2010
        POP/CON-RED-EX2010.contoso-lab.com
        POP3/CON-RED-EX2010
        POP3/CON-RED-EX2010.contoso-lab.com
        IMAP/CON-RED-EX2010
        IMAP/CON-RED-EX2010.contoso-lab.com
        IMAP4/CON-RED-EX2010
        IMAP4/CON-RED-EX2010.contoso-lab.com
        exchangeRFR/CON-RED-EX2010
        exchangeRFR/CON-RED-EX2010.contoso-lab.com
        exchangeAB/CON-RED-EX2010
        exchangeAB/CON-RED-EX2010.contoso-lab.com
        exchangeMDB/CON-RED-EX2010.contoso-lab.com
        exchangeMDB/CON-RED-EX2010
        SMTP/CON-RED-EX2010
        SMTP/CON-RED-EX2010.contoso-lab.com
        SmtpSvc/CON-RED-EX2010
        SmtpSvc/CON-RED-EX2010.contoso-lab.com
        WSMAN/CON-RED-EX2010
        WSMAN/CON-RED-EX2010.contoso-lab.com
        RestrictedKrbHost/CON-RED-EX2010
        HOST/CON-RED-EX2010
        RestrictedKrbHost/CON-RED-EX2010.contoso-lab.com
        HOST/CON-RED-EX2010.contoso-lab.com
```

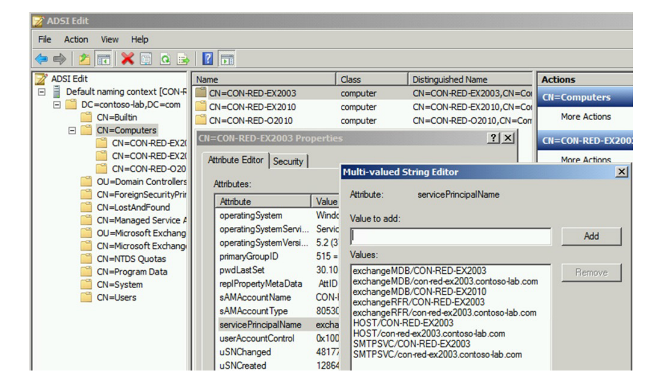
Setspn –X sucht nach Duplikaten:

```
C:\Users\Administrator>setspn -x
Checking domain DC=contoso-lab,DC=com
Processing entry 0
found 0 group of duplicate SPNs.
```

```
C:\Users\Administrator>setspn -x
Checking domain DC=contoso-lab,DC=com
Processing entry 0
exchangeMDB/CON-RED-EX2010 is registered on these accounts:
        CN=CON-RED-EX2003,CN=Computers,DC=contoso-lab,DC=com
        CN=CON-RED-EX2010,CN=Computers,DC=contoso-lab,DC=com

found 1 group of duplicate SPNs.
```

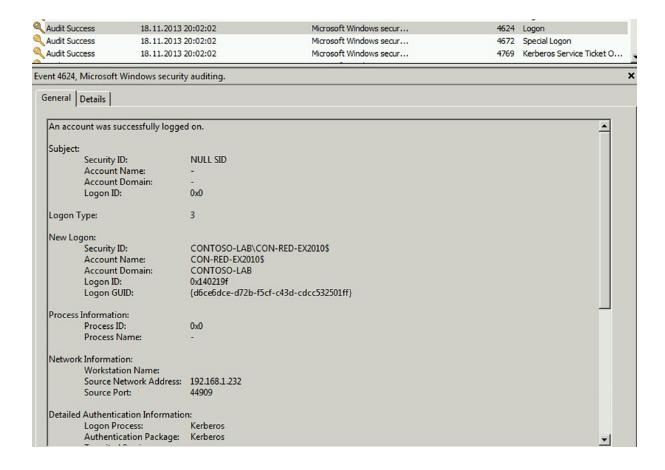
Da der SPN ein Attribut der Accounts in AD ist, kann auch ADSIEdit verwendet werden, um SPNs zu erstellen oder zu löschen:

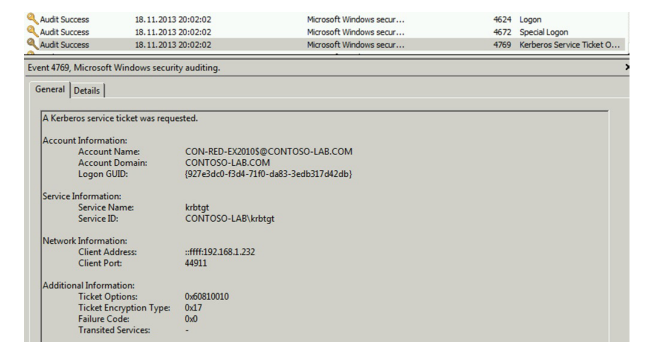


Ebenfalls hilfreich ist das Security Eventlog. In diesem lassen sich je nach Einstellung von Audit und Kerberos Debugging rudimentäre oder sehr detaillierte Informationen

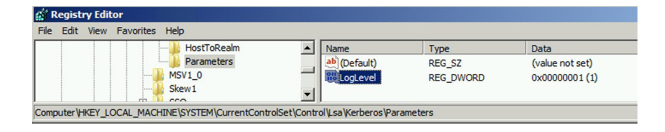


über erfolgreiche und fehlgeschlagene Authentisierungen gewinnen.

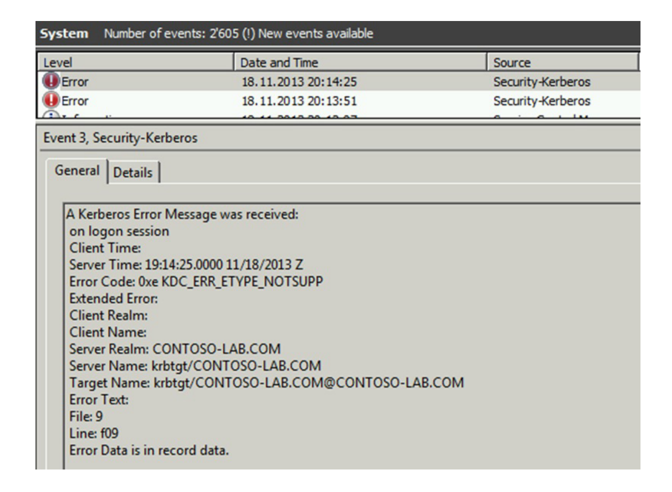




In Windows Server 2008 R2 lässt sich das Debug Logging für Kerberos in der Registrierung konfigurieren:



Der Key LogLevel existiert standardmässig nicht und muss erstellt werden. Dadurch werden zwar mehr Informationen geloggt, aber Achtung: Es gibt auch viele Events, die kein Problem darstellen und zu erwarten sind:



Fazit

Obwohl die Authentisierung in Active Directory üblicherweise ohne zusätzlichen Aufwand funktioniert, ist es ratsam, sicherzustellen, dass Kerberos statt NTLM verwendet wird. Dazu stehen diverse Hilfsmittel zur Verfügung. Voraussetzung, um diese auch verwenden zu können, ist ein Verständnis der Funktionsweise der Authentisierungsverfahren.